On a Generalisation of a Lehmer Problem

IGOR E. SHPARLINSKI
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

February 2, 2008

Abstract

We consider a generalisation of the classical Lehmer problem about the distribution of modular inverses in arithmetic progression, introduced by E. Alkan, F. Stan and A. Zaharescu. Using bounds of sums of multiplicative characters instead of traditionally applied to this kind of problem Kloosterman sums, we improve their results in several directions.

1 Introduction

Given modulus $q \geq 2$, we denote by $\mathcal{U}_q$ the set

$$\mathcal{U}_q = \{n \ : \ 1 \leq n < q, \ \gcd(n, q) = 1\}.$$

that is, $\#\mathcal{U}_q = \varphi(q)$, the Euler function.

For $n \in \mathcal{U}_q$ we use $\overline{n}$ to denote the modular inverse of n, that is, $n\overline{n} \equiv 1 \pmod q$, $\overline{n} \in \mathcal{U}_q$.

The classical question of D. H. Lehmer (see [9, Problem F12]) about the joint distribution of the parity of n and $\overline{n}$ has been solved by W. Zhang [19, 20].

Recently this question has been generalised by E. Alkan, F. Stan and A. Zaharescu [1] as follows. Given vector $\mathbf{a} = (a_1, \ldots, a_{k+1}) \in \mathcal{U}_q^{k+1}$ and

$\mathbf{b} = (b_1, \ldots, b_{k+1}) \in \mathbb{Z}^{k+1}$ we consider the set $\mathcal{N}(\mathbf{a}, \mathbf{b}, q)$ of vectors $\mathbf{n} = (n_1, \ldots, n_k) \in \mathcal{U}_q^k$ such that

$$\begin{aligned} n_i &\equiv b_i \pmod{a_i}, \qquad i = 1, \ldots, k, \\ \overline{n_1 \ldots n_k} &\equiv b_{k+1} \pmod{a_{k+1}}. \end{aligned}$$

Generalising several previous results of various authors, (for instance, of [3, 19, 20, 21]), E. Alkan, F. Stan and A. Zaharescu [1] have shown that for any fixed k, the bound

$$\#\mathcal{N}(\mathbf{a}, \mathbf{b}, q) = \frac{\varphi(q)^k}{a_1 \ldots a_{k+1}} + O(q^{k-1/2+o(1)}) \qquad (1)$$

holds uniformly over all vectors $\mathbf{a} \in \mathcal{U}_q^{k+1}$ and $\mathbf{b} \in \mathbb{Z}^{k+1}$. In particular, since

$$\varphi(q) \geq c \frac{q}{\log\log(q+2)} \qquad (2)$$

for an absolute constant $c > 0$, see [17, Section I.5.4], we see that the bound (1) is nontrivial for

$$a_1 \ldots a_{k+1} \leq q^{1/2-\delta} \qquad (3)$$

for any fixed $\delta > 0$, provided that q is large enough.

The main tool of [1] are bounds of exponential sum, in particular, multidimensional Kloosterman sums. Here we show that using bounds of multiplicative character sums, such the classical Polya-Vinogradov and Burgess bounds, see [10, Theorems 12.5 and 12.6], one can improve the bound (1). For example, we obtain a bound, which in particular implies that

$$\#\mathcal{N}(\mathbf{a}, \mathbf{b}, q) = \frac{\varphi(q)^k}{a_1 \ldots a_{k+1}} + O\left(\frac{\|\mathbf{a}\| q^{k-1+o(1)}}{a_1 \ldots a_{k+1}} + \frac{q^{(k+1)/2+o(1)}}{(a_1 \ldots a_{k+1})^{1/(k+1)}}\right), \qquad (4)$$

where $\|\mathbf{a}\|$ is the Euclidean norm of $\mathbf{a}$, which is equivalent to (1) for $k = 2$ and $\|\mathbf{a}\| = O(1)$ and always improves it if either $\|\mathbf{a}\|$ grows together with q or if $k \geq 3$ (in this case, with respect to both dependence on q and $\mathbf{a}$).

We note that instead of (3), the bound of our Theorem 8 is nontrivial when simultaneously

$$\|\mathbf{a}\| \leq q^{1-\delta} \quad \text{and} \quad a_1 \ldots a_{k+1} \leq \begin{cases} q^{(k^2-1)/2k-\delta} & \text{if } 2 \leq k \leq 4, \\ q^{5/2-\delta} & \text{if } k = 5, \\ q^{2(k^2-1)/3(k+2)-\delta} & \text{if } k \geq 6, \end{cases} \qquad (5)$$

for any fixed $\delta > 0$, provided that q is large enough. In fact we consider a more general case when $n_1, \ldots, n_k$ and $\overline{n_1 \ldots n_k}$ belong to a certain box inside of the cube $\mathbb{T}_{k+1}$, where

$$\mathbb{T}_s = (\mathbb{R}/\mathbb{Z})^s = [0,1)^s$$

is the k-dimensional unit torus.

The question about the distribution of elements of $\mathcal{N}(\mathbf{a}, \mathbf{b}, q)$ in various regions of $\mathbb{T}_k$ has also been studied in [1]. For an arbitrary region $\Omega \subseteq \mathbb{T}_k$ we denote by $\mathcal{N}_\Omega(\mathbf{a}, \mathbf{b}, q)$, the set of vectors $\mathbf{n} \in \mathcal{N}(\mathbf{a}, \mathbf{b}, q)$ which belong to the dilated region $q\Omega$. Let $\lambda(\Omega)$ denote the Lebesgue measure of Ω. It has been show in [1] that for any fixed k and region $\Omega \subseteq \mathbb{T}_k$, with piecewise smooth boundary,

$$\#\mathcal{N}_\Omega(\mathbf{a}, \mathbf{b}, q) = \lambda(\Omega) \frac{\varphi(q)^k}{a_1 \ldots a_{k+1}} + O(q^{k-1/2(k+1)+o(1)}) \tag{6}$$

holds uniformly over all vectors $\mathbf{a} \in \mathcal{U}_q^{k+1}$ and $\mathbf{b} \in \mathbb{Z}^{k+1}$.

Here we show that using some bounds from [1] in a combination with some results of M. Laczkovich [14] and of H. Niederreiter and J. M. Wills [16], from the theory of uniformly distributed sequences leads to a better error term in the asymptotic formula (6).

Furthermore, we also consider a generalisation to the joint distribution of $n_1, \ldots, n_k$ and $\overline{n_1 \ldots n_k}$ in arbitrary regions. Namely given an arbitrary region $\Theta \subseteq \mathbb{T}_{k+1}$ we estimate the cardinality of $\mathcal{M}_\Theta(\mathbf{a}, \mathbf{b}, q)$, which is the set of vectors $(n_1, \ldots, n_k) \in \mathcal{N}(\mathbf{a}, \mathbf{b}, q)$ for which $(n_1, \ldots, n_k, \overline{n_1 \ldots n_k})$ belongs to the dilated region $q\Theta$.

Finally, in the case of prime $q = p$, we show that a result of A. Ayyad, T. Cochrane and Z. Zheng [2, Theorem 2] leads to some improvements.

We conclude with a short discussion of possible ways to improve our results and of some open problems.

Throughout the paper, the implied constants in the symbols 'O', and '$\ll$' may depend on integer parameters k and r and a region $\Omega \subseteq \mathbb{T}_k$. We recall that the notations $U = O(V)$ and $V \ll U$ are both equivalent to the assertion that the inequality $|U| \le cV$ holds for some constant $c > 0$.

2 Preparations

2.1 Character Sums

Let $\mathcal{X}_q$ be the set of all $\#\mathcal{X}_q = \varphi(q)$ multiplicative characters of q. We refer to [15] for definitions and basic properties of multiplicative characters such as $\chi(u) = 0$ for any $\chi \in \mathcal{X}_q$ if $\gcd(u, q) > 1$ In particular, we recall that for $u \in Z$,

$$\frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}_q} \chi(u) = \begin{cases} 1 & \text{if } u \equiv 1 \pmod q, \\ 0 & \text{otherwise,} \end{cases} \tag{7}$$

see [15, Theorem 5.4]. We also use χ_0 to denote the principal character.

In particular, we immediately see the following bound

Lemma 1. *For any integers K and L with $0 \le K < K + L \le q$, an integer $a \ge 1$ with $\gcd(a, q) = 1$ and an arbitrary integer b,*

$$\sum_{\chi \in \mathcal{X}_q} \left| \sum_{\substack{K+1 \le n \le K+L \\ n \equiv b \pmod a}} \chi(n) \right|^2 \le \varphi(q)\,(L/a + 1)\,.$$

Proof. We recall that if $\gcd(n, q) = 1$ for the conjugated character $\overline{\chi}$ we have $\overline{\chi}(n) = \chi(\overline{n})$. Therefore

$$\begin{aligned} \sum_{\chi \in \mathcal{X}_q} \left| \sum_{\substack{K+1 \le n \le K+L \\ n \equiv b \pmod a}} \chi(n) \right|^2 &= \sum_{\chi \in \mathcal{X}_q} \left| \sum_{\substack{K+1 \le n \le K+L \\ n \equiv b \pmod a \\ \gcd(n,q)=1}} \chi(n) \right|^2 \\ &= \sum_{\chi \in \mathcal{X}_q} \sum_{\substack{K+1 \le n \le K+L \\ n \equiv b \pmod a \\ \gcd(n,q)=1}} \sum_{\substack{K+1 \le m \le K+L \\ m \equiv b \pmod a \\ \gcd(m,q)=1}} \chi(n)\,\chi(\overline{m}) \\ &= \sum_{\substack{K+1 \le n \le K+L \\ n \equiv b \pmod a \\ \gcd(n,q)=1}} \sum_{\substack{K+1 \le m \le K+L \\ m \equiv b \pmod a \\ \gcd(m,q)=1}} \sum_{\chi \in \mathcal{X}_q} \chi(n\overline{m}) = \varphi(q) T, \end{aligned}$$

where T is the number of pairs (n, m) with

$$\begin{aligned} K + 1 \le m, n \le K + L, \qquad & m \equiv n \equiv b \pmod a, \\ \gcd(mn, q) = 1, \qquad & m \equiv n \pmod q. \end{aligned}$$

Clearly n takes at most $L/a+1$ possible values and since $0 \le K < K+L \le q$, for each n the value of m is uniquely defined. Therefore $T \le L/a+1$, which concludes the proof. □

The following result is a combination of the Polya-Vinogradov bound (for $r=1$) and Burgess (for $r \ge 2$) bounds, see [10, Theorems 12.5 and 12.6].

Lemma 2. *For any positive integers U and $V \le q$, the bound*

$$\max_{\substack{\chi \in \mathcal{X}_q \\ \chi \neq \chi_0}} \left| \sum_{n=U+1}^{U+V} \chi(n) \right| \le V^{1-1/r} q^{(r+1)/4r^2+o(1)}.$$

holds with $r = 1,2,3$ for any q and with arbitrary integer r if $q = p$ is prime.

Now, using the identity

$$\begin{aligned} \sum_{\substack{K+1 \le n \le K+L \\ n \equiv b \pmod a}} \chi(n) &= \sum_{K+1 \le am+b \le K+L} \chi(am+b) \\ &= \chi(a) \sum_{(K+1-b)/a \le m \le (K+L-b)/a} \chi(m+b\overline{a}) \end{aligned} \tag{8}$$

we derive from Lemma 2 the following useful estimate.

Lemma 3. *For any positive integers K, L and $a \ge L$ such that* $\gcd(a,q)=1$ *and an arbitrary integer b, the bound*

$$\max_{\substack{\chi \in \mathcal{X}_q \\ \chi \neq \chi_0}} \left| \sum_{\substack{K+1 \le n \le K+L \\ n \equiv b \pmod a}} \chi(n) \right| \le q^{(4r^2-3r+1)/4r^2+o(1)} a^{-(r-1)/r}$$

holds with $r = 1,2,3$ for any q and with arbitrary integer r is $q = p$ is prime.

We also need to approximate the value of the sum of Lemma 3 with the principal character χ_0.

We denote by $\omega(q)$ the number of prime divisors of q.

Lemma 4. *For any positive integers K and L, an integer $a \ge 1$ such that* $\gcd(a,q)=1$ *and an arbitrary integer b,*

$$\sum_{\substack{K+1 \le n \le K+L \\ n \equiv b \pmod a}} \chi_0(n) = \frac{\varphi(q)L}{aq} + O(2^{\omega(q)}).$$

Proof. Clearly

$$\sum_{\substack{K+1\le n\le K+L\\ n\equiv b \pmod a}} \chi_0(n) = \sum_{\substack{K+1\le am+b\le K+L\\ \gcd(am+b,q)=1}} 1.$$

Using the Möbius function $\mu(d)$ over the divisors of q to detect the coprimality condition and interchanging the order of summation, we obtain

$$\sum_{\substack{K+1\le am+b\le K+L\\ \gcd(am+b,q)=1}} 1 = \sum_{d|q} \mu(d)\left(\frac{L}{da} + O(1)\right) = \frac{L}{a}\sum_{d|q}\frac{\mu(d)}{d} + O\left(\sum_{d|q}|\mu(d)|\right)$$

from which the result follows immediately. □

Finally, if $q = p$ then we also use the following bound which follows from a result of A. Ayyad, T. Cochrane and Z. Zheng [2, Theorem 2] and the identity (8).

Lemma 5. *Let $q = p$ be prime. For any integers K and L with $0 \le K < K + L \le p$, an integer $a \ge 1$ with $\gcd(a,p) = 1$ and an arbitrary integer b,*

$$\sum_{\substack{\chi\in\mathcal{X}_p\\ \chi\ne\chi_0}} \left| \sum_{\substack{K+1\le n\le K+L\\ n\equiv b \pmod a}} \chi(n) \right|^4 \ll p(L/a+1)^2(\log p)^2.$$

2.2 Discrepancy

For a finite set $\mathcal{F} \subseteq \mathbb{T}_s$ of the unit s-dimensional set, we define its *discrepancy with respect to a domain* $\Xi \subseteq \mathbb{T}_s$ as

$$\Delta(\mathcal{F},\Xi) = \left| \frac{\#\{\mathbf{f}\in\mathcal{A}:\ \mathbf{f}\in\Xi\}}{\#\mathcal{F}} - \lambda(\Xi) \right|,$$

where, as before, λ is the Lebesgue measure on $\mathbb{T}_s$.

We now define the *discrepancy* of $\mathcal{F}$ as

$$D(\mathcal{F}) = \sup_{\Pi\subseteq\mathbb{T}_s} \Delta(\mathcal{F},\Pi),$$

where the supremum is taken over all boxes $\Pi = [\alpha_1,\beta_1) \times \ldots \times [\alpha_s,\beta_s)$.

As usual, we define the distance between a vector $\mathbf{u} \in \mathbb{T}_s$ and a set $\mathit{\Gamma} \subseteq \mathbb{T}_s$ by

$$\mathrm{dist}(\mathbf{u}, \mathit{\Gamma}) = \inf_{\mathbf{w} \in \mathit{\Gamma}} \|\mathbf{u} - \mathbf{w}\|,$$

where, as before, $\|\mathbf{v}\|$ denotes the Euclidean norm of $\mathbf{v}$. Given $\varepsilon > 0$ and a domain $\mathit{\Xi} \subseteq \mathbb{T}_s$ we define the sets

$$\mathit{\Xi}_\varepsilon^+ = \{\mathbf{u} \in \mathbb{T}_s \backslash \mathit{\Xi} \mid \mathrm{dist}(\mathbf{u}, \mathit{\Xi}) < \varepsilon\}$$

and

$$\mathit{\Xi}_\varepsilon^- = \{\mathbf{u} \in \mathit{\Xi} \mid \mathrm{dist}(\mathbf{u}, \mathbb{T}_s \backslash \mathit{\Xi}) < \varepsilon\}.$$

Let $h(\varepsilon)$ be an arbitrary increasing function defined for $\varepsilon > 0$ and such that

$$\lim_{\varepsilon \to 0} h(\varepsilon) = 0.$$

As in [14, 16], we define the class $\mathcal{S}_h$ of domains $\mathit{\Xi} \subseteq \mathbb{T}_s$ for which

$$\lambda\left(\mathit{\Xi}_\varepsilon^+\right) \le h(\varepsilon) \qquad \text{and} \qquad \lambda\left(\mathit{\Xi}_\varepsilon^-\right) \le h(\varepsilon).$$

A relation between $D(\mathcal{F})$ and $\mathit{\Delta}(\mathcal{F}, \mathit{\Xi})$ for $\mathit{\Xi} \in \mathcal{S}_h$ is given by the following inequality of M. Laczkovich [14] (see also [16]).

Lemma 6. *For any domain $\mathit{\Xi} \in \mathcal{S}_h$, we have*

$$\mathit{\Delta}(\mathcal{F}, \mathit{\Xi}) \ll h\left(s^{1/2} D(\mathcal{F})^{1/s}\right).$$

Finally, the following bound, which is a partial case of a more general result of H. Weyl [18] shows that if $\mathit{\Xi}$ has a piecewise smooth boundary that $\mathit{\Xi} \in \mathcal{S}_h$ for some linear function $h(\varepsilon) = C\varepsilon$.

Lemma 7. *For any domain $\mathit{\Xi} \in \mathcal{S}_h$ with piecewise smooth boundary, we have*

$$\lambda\left(\mathit{\Xi}_\varepsilon^\pm\right) = O(\varepsilon).$$

3 Main Results

3.1 Distribution in Boxes

Here we study $\mathcal{M}_\Theta(\mathbf{a}, \mathbf{b}, q)$ in the case where $\Theta = \mathit{\Sigma}$ is a box $\mathit{\Sigma} \subseteq \mathbb{T}_{k+1}$ and in particular we generalise and improve the bound (1).

We recall that we use $\|\mathbf{a}\|$ to denote the Euclidean norm of $\mathbf{a} \in \mathcal{U}_q^{k+1}$.

Theorem 8. *For $r = 1, 2, 3$, any fixed $k \ge 2$, and a box*

$$\varSigma = [\alpha_1, \beta_1) \times \ldots \times [\alpha_{k+1}, \beta_{k+1}) \subseteq \mathbb{T}_{k+1}$$

the bound

$$\begin{aligned}\#\mathcal{M}_{\varSigma}(\mathbf{a}, \mathbf{b}, q) = \lambda(\varSigma)&\frac{\varphi(q)^k}{a_1 \ldots a_{k+1}} \\ &+O\left(\frac{\|\mathbf{a}\| q^{k-1+o(1)}}{a_1 \ldots a_{k+1}} + \frac{q^{k-(3r-1)(k-1)/4r^2+o(1)}}{(a_1 \ldots a_{k+1})^{1-(k+r-1)/r(k+1)}}\right)\end{aligned}$$

holds uniformly over all vectors $\mathbf{a} \in \mathcal{U}_q^{k+1}$ and $\mathbf{b} \in \mathbb{Z}^{k+1}$.

Proof. We see from (7) that

$$\begin{aligned}\#\mathcal{M}_{\varSigma}(\mathbf{a}, \mathbf{b}, q) = \sum_{\substack{\alpha_1 q \le n_1 < \beta_1 q \\ n_1 \equiv b_1 \pmod{a_1}}} \ldots \sum_{\substack{\alpha_{k+1} q \le n_{k+1} < \beta_{k+1} q \\ n_{k+1} \equiv b_{k+1} \pmod{a_{k+1}}}}& \\ \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}_q} \chi\left(n_1 \ldots n_{k+1}\right).&\end{aligned}$$

We now change the order of summation and note that by Lemma 4 the term corresponding to the principal character $\chi = \chi_0$ is equal to

$$\begin{aligned}\frac{1}{\varphi(q)} \sum_{\substack{\alpha_1 q \le n_1 < \beta_1 q \\ n_1 \equiv b_1 \pmod{a_1} \\ \gcd(n_1, q) = 1}} \ldots \sum_{\substack{\alpha_{k+1} q \le n_{k+1} < \beta_{k+1} q \\ n_{k+1} \equiv b_{k+1} \pmod{a_{k+1}} \\ \gcd(n_{k+1}, q) = 1}} 1& \\ = \frac{1}{\varphi(q)} \prod_{\nu=1}^{k+1} \left(\frac{(\beta_\nu - \alpha_\nu)\varphi(q)}{a_\nu} + O\left(2^{\omega(q)}\right)\right)& \\ = \lambda(\varSigma)\frac{\varphi(q)^k}{a_1 \ldots a_{k+1}} + O\left(\frac{\|\mathbf{a}\| \varphi(q)^{k-1}}{a_1 \ldots a_{k+1}} 2^{k\omega(q)}\right)& \\ = \lambda(\varSigma)\frac{\varphi(q)^k}{a_1 \ldots a_{k+1}} + O\left(\frac{\|\mathbf{a}\| q^{k-1+o(1)}}{a_1 \ldots a_{k+1}}\right),&\end{aligned}$$

since

$$\omega(q) \ll \frac{\log q}{\log\log q},$$

see [17, Section I.5.3], and the bound (2). Hence,

$$\#\mathcal{M}_{\varSigma}(\mathbf{a},\mathbf{b},q) = \lambda(\varSigma)\frac{\varphi(q)^k}{a_1\ldots a_{k+1}} + O\left(\frac{\|\mathbf{a}\|q^{k-1+o(1)}}{a_1\ldots a_{k+1}} + R\right), \qquad (9)$$

where

$$\begin{aligned} R &= \frac{1}{\varphi(q)}\sum_{\substack{\chi\in\mathcal{X}_q\\ \chi\neq\chi_0}}\ \sum_{\substack{\alpha_1 q\le n_1<\beta_1 q\\ n_1\equiv b_1 \pmod{a_1}}}\ \ldots \sum_{\substack{\alpha_{k+1} q\le n_{k+1}<\beta_{k+1} q\\ n_{k+1}\equiv b_{k+1} \pmod{a_{k+1}}}} \chi\left(n_1\ldots n_{k+1}\right) \\ &= \frac{1}{\varphi(q)}\sum_{\substack{\chi\in\mathcal{X}_q\\ \chi\neq\chi_0}}\prod_{\nu=1}^{k+1}\ \sum_{\substack{\alpha_\nu q\le n_\nu<\beta_\nu q\\ n_\nu\equiv b_\nu \pmod{a_\nu}}} \chi\left(n_\nu\right). \end{aligned}$$

Thus using the Hölder inequality we obtain

$$R^{k+1} \le \frac{1}{\varphi(q)^{k+1}}\prod_{\nu=1}^{k+1}\sum_{\substack{\chi\in\mathcal{X}_q\\ \chi\neq\chi_0}}\left|\sum_{\substack{\alpha_\nu q\le n_\nu<\beta_\nu q\\ n_\nu\equiv b_\nu \pmod{a_\nu}}} \chi\left(n_\nu\right)\right|^{k+1}. \qquad (10)$$

Since the bound is trivial for $\|\mathbf{a}\| \ge q$, we can assume that

$$\max\{a_1,\ldots,a_{k+1}\} < q.$$

Applying Lemma 3 to the $(k-1)$th power of the character sums for each $\nu = 1,\ldots,k+1$, and then extending the summation over all characters $\chi \in \mathcal{X}$, we obtain that for $r = 1, 2, 3$

$$\begin{aligned} &\sum_{\substack{\chi\in\mathcal{X}_q\\ \chi\neq\chi_0}}\left|\sum_{\substack{\alpha_\nu q\le n_\nu<\beta_\nu q\\ n_\nu\equiv b_\nu \pmod{a_\nu}}} \chi\left(n_\nu\right)\right|^{k+1} \\ &\qquad \le \left(q^{(4r^2-3r+1)/4r^2+o(1)}a_\nu^{-(r-1)/r}\right)^{k-1}\sum_{\chi\in\mathcal{X}_q}\left|\sum_{\substack{\alpha_\nu q\le n_\nu<\beta_\nu q\\ n_\nu\equiv b_\nu \pmod{a_\nu}}} \chi\left(n_\nu\right)\right|^{2}. \end{aligned}$$

We now use Lemma 1, which implies

$$\begin{aligned}\sum_{\chi \in \mathcal{X}_q} \left| \sum_{\substack{\alpha_\nu q \le n_\nu < \beta_\nu q \\ n_\nu \equiv b_\nu \pmod{a_\nu}}} \chi\left(n_\nu\right) \right|^{k+1} & \le \left(q^{(4r^2-3r+1)/4r^2+o(1)} a_\nu^{-(r-1)/r} \right)^{k-1} q^2 a_\nu^{-1} \\ & \le q^{(k+1)-(3r-1)(k-1)/4r^2+o(1)} a_\nu^{-(rk-k+1)/r}.\end{aligned}$$

Substituting this bound in (10) and using (2), we obtain

$$R \le q^{k-(3r-1)(k-1)/4r^2+o(1)} \left(\prod_{\nu=1}^{k+1} a_\nu \right)^{-(rk-k+1)/r(k+1)},$$

which together with (9) completes the proof. □

In particular, taking $r = 3$ we see that the bound of Theorem 8 implies that for any fixed k and $\delta > 0$ there exists $\eta > 0$ such that under the conditions (5) we have

$$\#\mathcal{M}_\Sigma(\mathbf{a}, \mathbf{b}, q) = \left(\lambda(\Sigma) + O(q^{-\eta}) \right) \frac{\varphi(q)^k}{a_1 \ldots a_{k+1}}.$$

Moreover, using the trivial bounds

$$\|\mathbf{a}\| \le a_1 \ldots a_{k+1} \qquad \text{and} \qquad (a_1 \ldots a_{k+1})^{1/(k+1)} \ge 1,$$

we derive from Theorem 8 that

$$\#\mathcal{M}_\Sigma(\mathbf{a}, \mathbf{b}, q) = \lambda(\Sigma) \frac{\varphi(q)^k}{a_1 \ldots a_{k+1}} + O\left(q^{k-1+o(1)} + q^{(k+1)/2+o(1)} \right).$$

Finally, taking $\Sigma = \mathbb{T}_{k+1}$ and $r = 1$ in Theorem 8, we obtain (4).

3.2 Distribution in General Regions

Here we give an improvement and generalisation of the asymptotic formula (6).

Theorem 9. *For $r = 1, 2, 3$, any fixed $k \geq 2$ and region $\varTheta \subseteq \mathbb{T}_{k+1}$ with piecewise smooth boundary,*

$$\#\mathcal{M}_{\varTheta}(\mathbf{a}, \mathbf{b}, q) = \lambda(\varTheta)\frac{\varphi(q)^k}{a_1 \dots a_{k+1}} + O\left(\frac{\|\mathbf{a}\|^{1/(k+1)} q^{k-1/(k+1)+o(1)}}{a_1 \dots a_{k+1}} + \frac{q^{k-(3r-1)(k-1)/4r^2(k+1)+o(1)}}{(a_1 \dots a_{k+1})^{1-(k+r-1)/r(k+1)^2}}\right)$$

holds uniformly over all vectors $\mathbf{a} \in \mathcal{U}_q^{k+1}$ and $\mathbf{b} \in \mathbb{Z}^{k+1}$.

Proof. It follows from Theorem 8 and the estimates (2) and (4) that we have the bound

$$D(\mathcal{A}(\mathbf{a}, \mathbf{b}, q)) \ll \|\mathbf{a}\| q^{-1+o(1)} + (a_1 \dots a_{k+1})^{(r+k-1)/r(k+1)} q^{-(3r-1)(k-1)/4r^2+o(1)}$$

on the box discrepancy of the set

$$\mathcal{A}(\mathbf{a}, \mathbf{b}, q) = \left\{ \left(\frac{n_1}{q}, \dots, \frac{n_k}{q}, \frac{\overline{n_1 \dots n_k}}{q} \right) \ : (n_1, \dots, n_k) \in \mathcal{N}(\mathbf{a}, \mathbf{b}, q) \right\}.$$

Therefore, by Lemma 6 and Lemma 7 we conclude that the discrepancy of $\mathcal{A}(\mathbf{a}, \mathbf{b}, q)$ with respect to $\varTheta$ satisfies

$$\varDelta(\mathcal{A}(\mathbf{a}, \mathbf{b}, q), \varTheta) \ll \|\mathbf{a}\|^{1/(k+1)} q^{-1/(k+1)+o(1)} + (a_1 \dots a_{k+1})^{k/r(k+1)^2} q^{-(3r-1)(k-1)/4r^2(k+1)+o(1)}$$

which is equivalent to the desired result. □

Certainly applying Theorem 9 with $\varTheta = \varOmega \times [0, 1)$ where $\varOmega \subseteq \mathbb{T}_k$ one immediately obtains an asymptotic formula for $\mathcal{N}_{\varOmega}(\mathbf{a}, \mathbf{b}, q)$ (which is already stronger than (6). However since the problem of estimating $\mathcal{N}_{\varOmega}(\mathbf{a}, \mathbf{b}, q)$ is of lower dimension (k instead of $k + 1$) one obtains a slightly stronger bound in this case.

Theorem 10. *For $r = 1, 2, 3$, any fixed $k \geq$ and region $\varOmega \subseteq \mathbb{T}_k$ with piecewise smooth boundary,*

$$\#\mathcal{N}_{\varOmega}(\mathbf{a}, \mathbf{b}, q) \quad = \quad \lambda(\varOmega)\frac{\varphi(q)^k}{a_1 \dots a_{k+1}} + O\left(\frac{\|\mathbf{a}\|^{1/k} q^{k-1/k+o(1)}}{a_1 \dots a_{k+1}} + \frac{q^{k-(3r-1)(k-1)/4r^2k+o(1)}}{(a_1 \dots a_{k+1})^{1-(k+r-1)/rk(k+1)}}\right)$$

holds uniformly over all vectors $\mathbf{a} \in \mathcal{U}_q^{k+1}$ and $\mathbf{b} \in \mathbb{Z}^{k+1}$.

Proof. Taking the box $\Sigma = \Pi \times [0,1)$, where a box $\Pi \subseteq \mathbb{T}_k$ we see that it follows from Theorem 8 and the estimates (2) and (4) that we have the bound

$$D(\mathcal{B}(\mathbf{a},\mathbf{b},q)) \ll \|\mathbf{a}\| q^{-1+o(1)} + (a_1 \ldots a_{k+1})^{(r+k-1)/r(k+1)} q^{-(3r-1)(k-1)/4r^2+o(1)}$$

on the box discrepancy of the set

$$\mathcal{B}(\mathbf{a},\mathbf{b},q) = \left\{ \left(\frac{n_1}{q}, \ldots, \frac{n_k}{q} \right) \ : (n_1, \ldots, n_k) \in \mathcal{N}(\mathbf{a},\mathbf{b},q) \right\}.$$

that is, of the same strength as that for the set $\mathcal{A}(\mathbf{a},\mathbf{b},q)$ in the proof of Theorem 9.

Therefore, by Lemma 6 and Lemma 7 we conclude that the discrepancy of $\mathcal{B}(\mathbf{a},\mathbf{b},q)$ with respect to Ω satisfies

$$\begin{aligned} &\Delta(\mathcal{B}(\mathbf{a},\mathbf{b},q), \Omega) \\ &\qquad \ll \|\mathbf{a}\|^{1/k} q^{-1/k+o(1)} + (a_1 \ldots a_{k+1})^{(r+k-1)/rk(k+1)} q^{-(3r-1)(k-1)/4r^2k+o(1)} \end{aligned}$$

which is equivalent to the desired result. □

We remark that although in the case of $k = 2$ and fixed $\mathbf{a}$, Theorem 8 (with the optimal choice of $r = 1$) is equivalent to (1), the bound of Theorem 10 still improves (6) due to our use of Lemma 6 instead of the arguments from [1].

3.3 Some Improvements for Prime $q = p$

Here we show that if $q = p$ is prime and $k \geq 3$ then using Lemma 5 instead of Lemma 1 leads to a stronger bounds wit respect to the product $a_1 \ldots a_{k+1}$.

Theorem 11. *Let $q = p$ be prime. For any fixed integer $r \geq 1$ and $k \geq 3$, and a box*

$$\Sigma = [\alpha_1, \beta_1) \times \ldots \times [\alpha_{k+1}, \beta_{k+1}) \subseteq \mathbb{T}_{k+1}$$

the bound

$$\begin{aligned} \#\mathcal{M}_\Sigma(\mathbf{a},\mathbf{b},p) = \lambda(\Sigma) &\frac{p^k}{a_1 \ldots a_{k+1}} \\ &+ O\left(\frac{\|\mathbf{a}\| p^{k-1+o(1)}}{a_1 \ldots a_{k+1}} + \frac{p^{k-(3r-1)(k-3)/4r^2+o(1)}}{(a_1 \ldots a_{k+1})^{1-(k+2r-3)/r(k+1)}} \right) \end{aligned}$$

holds uniformly over all vectors $\mathbf{a} \in \mathcal{U}_q^{k+1}$ and $\mathbf{b} \in \mathbb{Z}^{k+1}$.

Proof. We proceed as in the proof of Theorem 8 and also note that one can change $(p-1)^k$ to p^k in (9) without changing the error term. In particular, we still have (10). Again as in the proof of Theorem 8 we apply Lemma 3, however this time to the $(k-3)$th power of the character sums for each $\nu = 1, \ldots, k+1$ (and this time we do not extend the summation over all characters $\chi \in \mathcal{X}$), we obtain that for any integer $r \geq 1$

$$\sum_{\substack{\chi \in \mathcal{X}_p \\ \chi \neq \chi_0}} \left| \sum_{\substack{\alpha_\nu p \leq n_\nu < \beta_\nu p \\ n_\nu \equiv b_\nu \pmod{a_\nu}}} \chi\left(n_\nu\right) \right|^{k+1}$$
$$\leq \left(p^{(4r^2-3r+1)/4r^2+o(1)} a_\nu^{-(r-1)/r}\right)^{k-3} \sum_{\substack{\chi \in \mathcal{X}_p \\ \chi \neq \chi_0}} \left| \sum_{\substack{\alpha_\nu p \leq n_\nu < \beta_\nu p \\ n_\nu \equiv b_\nu \pmod{a_\nu}}} \chi\left(n_\nu\right) \right|^{4}.$$

We now use Lemma 5, which implies

$$\begin{aligned} \sum_{\substack{\chi \in \mathcal{X}_p \\ \chi \neq \chi_0}} \left| \sum_{\substack{\alpha_\nu p \leq n_\nu < \beta_\nu p \\ n_\nu \equiv b_\nu \pmod{a_\nu}}} \chi\left(n_\nu\right) \right|^{k+1} &\leq \left(p^{(4r^2-3r+1)/4r^2+o(1)} a_\nu^{-(r-1)/r}\right)^{k-3} p^4 a_\nu^{-2} \\ &\leq p^{k+1-(3r-1)(k-3)/4r^2+o(1)} a_\nu^{-(rk-k-r+3)/r(k+1)}. \end{aligned}$$

Substituting this bound in (10) and using (2), we obtain

$$R \leq p^{k-(3r-3)(k-1)/4r^2+o(1)} \left(\prod_{\nu=1}^{k+1} a_\nu\right)^{-(rk-k-r+3)/r(k+1)},$$

which together with (9) completes the proof. □

In particular we see that the bound of Theorem 11 taken with $r = 1$ implies that for any fixed k and $\delta > 0$ there exists $\eta > 0$ such that under the conditions

$$\|\mathbf{a}\| \leq p^{1-\delta} \qquad \text{and} \qquad a_1 \ldots a_{k+1} \leq p^{(k+1)/2-\delta}$$

we have

$$\#\mathcal{M}_{\Sigma}(\mathbf{a}, \mathbf{b}, p) = \left(\lambda(\Sigma) + O(p^{-\eta})\right) \frac{p^k}{a_1 \ldots a_{k+1}}.$$

However, taking a sufficiently large r we see from Theorem 11 that for any $\delta > 0$ there exists K_0 and $\eta > 0$ such that for $k \ge K_0$ the above bound holds under the condition

$$\|\mathbf{a}\| \le p^{1-\delta} \qquad \text{and} \qquad a_1 \dots a_{k+1} \le p^{(3/4-\delta)k}$$

We also have analogues of Theorems 9 and 10.

Theorem 12. *Let $q = p$ be prime. For any fixed integer $r \ge 1$ and $k \ge 3$, and region $\varTheta \subseteq \mathbb{T}_{k+1}$ with piecewise smooth boundary,*

$$\begin{aligned}\#\mathcal{M}_{\varTheta}(\mathbf{a}, \mathbf{b}, p) = \lambda(\varTheta)&\frac{p^k}{a_1 \dots a_{k+1}}\\ &+ O\left(\frac{\|\mathbf{a}\|^{1/(k+1)}p^{k-1/(k+1)+o(1)}}{a_1 \dots a_{k+1}} + \frac{p^{k-(3r-1)(k-3)/4r^2(k+1)+o(1)}}{(a_1 \dots a_{k+1})^{1-(k+2r-3)/r(k+1)^2}}\right)\end{aligned}$$

holds uniformly over all vectors $\mathbf{a} \in \mathcal{U}_q^{k+1}$ and $\mathbf{b} \in \mathbb{Z}^{k+1}$.

Theorem 13. *Let $q = p$ be prime. For any fixed integer $r \ge 1$ and $k \ge 3$, and region $\varOmega \subseteq \mathbb{T}_k$ with piecewise smooth boundary,*

$$\begin{aligned}\#\mathcal{N}_{\varOmega}(\mathbf{a}, \mathbf{b}, p) = \lambda(\varOmega)&\frac{p^k}{a_1 \dots a_{k+1}}\\ &+ O\left(\frac{\|\mathbf{a}\|^{1/k}p^{k-1/k+o(1)}}{a_1 \dots a_{k+1}} + \frac{p^{k-(3r-1)(k-3)/4r^2k+o(1)}}{(a_1 \dots a_{k+1})^{1-(k+2r-3)/rk(k+1)}}\right)\end{aligned}$$

holds uniformly over all vectors $\mathbf{a} \in \mathcal{U}_q^{k+1}$ and $\mathbf{b} \in \mathbb{Z}^{k+1}$.

4 Concluding Remarks

4.1 Further Improvements

Clearly, if some of $a_1, \dots, a_{k+1}$ are of different order magnitude, then in the proofs of Theorems 8 and 11 one can use Lemma 2 with various values of r for each ν which may lead to stronger bounds. However it seems that the optimal strategy of applying these results heavily depends on various relations between the sizes of $a_1, \dots, a_{k+1}$ and q.

We believe that there are several further possibilities of improving Theorem 8 and in particular improving the threshold (5). Certainly there should be a variant of the result of A. Ayyad, T. Cochrane and Z. Zheng [2, Theorem 2], given in Lemma 5, which holds for arbitrary composite moduli q (see also [4]). In fact, J. B. Friedlander and H. Iwaniec [7] give such a bound, but only for special intervals (starting at the origin). Certainly, obtaining such a general result is of independent interest. Furthermore, the technique used by M. Z. Garaev [8] can probably be useful as well.

We also note that by a result of H. Niederreiter and J. M. Wills [16] for the class of convex sets Θ and Ω the implied constants do not depend on the set (see also [5, Theorem 1.12] and [13, Theorem 1.6, Chapter 2]).

4.2 Some Open Problems

It is certainly interesting to study various geometric properties of the set $\mathcal{N}(\mathbf{a}, \mathbf{b}, q)$. For example, let

$$H(\mathbf{a}, \mathbf{b}, q) = \max_{(n_1, \ldots n_k) \in \mathcal{N}(\mathbf{a}, \mathbf{b}, q)} \min_{1 \le i \le k} \left| n_i - \overline{n_1 \ldots n_k} \right| .$$

For $k = 1$, $\mathbf{a} = (1, 1)$, $\mathbf{b} = (0, 0)$, the value of

$$H(q) = \max_{n \in \mathcal{U}_q} |n - \overline{n}|$$

has been studied in [6, 11]. In particular, it has been shown in [11] that $H(q) = q + O\left(q^{3/4+o(1)}\right)$. It has also been shown in [6] that $H(q)$ is influenced by the distribution of divisors of $qs - 1$ for small values of s, and thus some lower bounds on $H(q)$ have been derived. It would be interesting to find out whether the behavior of $H(\mathbf{a}, \mathbf{b}, q)$ is also influenced by some arithmetic properties of the modulus q.

Finally, one can also study various geometric properties of the convex closure of $\mathcal{N}(\mathbf{a}, \mathbf{b}, q)$. For example, for $k = 1$, $\mathbf{a} = (1, 1)$, $\mathbf{b} = (0, 0)$, that is, for the set

$$\mathcal{N}(q) = \{(n, \overline{n}) \ : \ n \in \mathcal{U}_q\}$$

some lower and upper bounds on the number of vertices $V(q)$ of its convex closure have been given in [12]. These bounds as well as some numerical calculations suggest that the convex closure of $\mathcal{N}(q)$ does not behave as the convex closure of a random set, but rather is affected by the arithmetic structure of $q-1$ (and probably of $qs-1$ for small integers s). It would be interesting to see whether the same effect appears in the behaviour of the convex closure of $\mathcal{N}(\mathbf{a},\mathbf{b},q)$ for larger values of k and "generic" vectors $\mathbf{a}$ and $\mathbf{b}$.

References

[1] E. Alkan, F. Stan and A. Zaharescu, 'Lehmer k-tuples', *Proc. Amer. Math. Soc.*, **134** (2006), 2807–2815.

[2] A. Ayyad, T. Cochrane and Z. Zheng, 'The congruence $x_1x_2 \equiv x_3x_4 \pmod p$, the equation $x_1x_2 = x_3x_4$ and the mean value of character sums', *J. Number Theory*, **59** (1996), 398–413.

[3] C. Cobeli and A. Zaharescu, 'Generalization of a problem of Lehmer', *Manuscr. Math.*, **104** (2001), 301–307.

[4] T. Cochrane and Z. Zheng, 'High order moments of character sums', *Proc. Amer. Math. Soc.*, **126** (1998), 951–956.

[5] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997.

[6] K. Ford, M. R. Khan, I. E. Shparlinski and C. L. Yankov, 'On the maximal difference between an element and its inverse in residue rings', *Proc. Amer. Math. Soc.*, **133** (2005), 3463–3468.

[7] J. B. Friedlander and H. Iwaniec, 'The divisor problem for arithmetic progressions', *Acta Arith.*, **45** (1985), 273–277.

[8] M. Z. Garaev, 'Character sums in short intervals and the multiplication table modulo a large prime', *Monatsh. Math.*, **148** (2006), 127–138.

[9] R. K. Guy, *Unsolved problems in number theory*, Springer-Verlag, New York, 1994.

[10] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[11] M. R. Khan and I. E. Shparlinski, 'On the maximal difference between an element and its inverse modulo n', *Period. Math. Hung.*, **47** (2003), 111–117.

[12] M. R. Khan, I. E. Shparlinski and C. L. Yankov, 'On the convex closure of the graph of modular inversions', *Preprint*, 2006.

[13] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience Publ., 1974.

[14] M. Laczkovich, 'Discrepancy estimates for sets with small boundary', *Studia Sci. Math. Hungar.*, **30** (1995), 105–109.

[15] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[16] H. Niederreiter and J. M. Wills, 'Diskrepanz und Distanz von Massen bezuglich konvexer und Jordanscher Mengen', *Math. Z.*, **144** (1975), 125–134.

[17] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Univ. Press, 1995.

[18] H. Weyl, 'On the volume of tubes', *Amer. J. Math.*, **61** (1939), 461–472.

[19] W. Zhang, 'On a problem of D. H. Lehmer and its generalization', *Compos. Math.*, **86** (1993), 307–316.

[20] W. Zhang, 'On a problem of D. H. Lehmer and its generalization, II', *Compos. Math.*, **91** (1994), 47–56.

[21] W. Zhang, 'On the difference between a D. H. Lehmer number and its inverse modulo q', *Acta Arith.*, **68** (1994), 255–263.